

Preventing Remote Cyber Attacks against Aircraft Avionics Systems

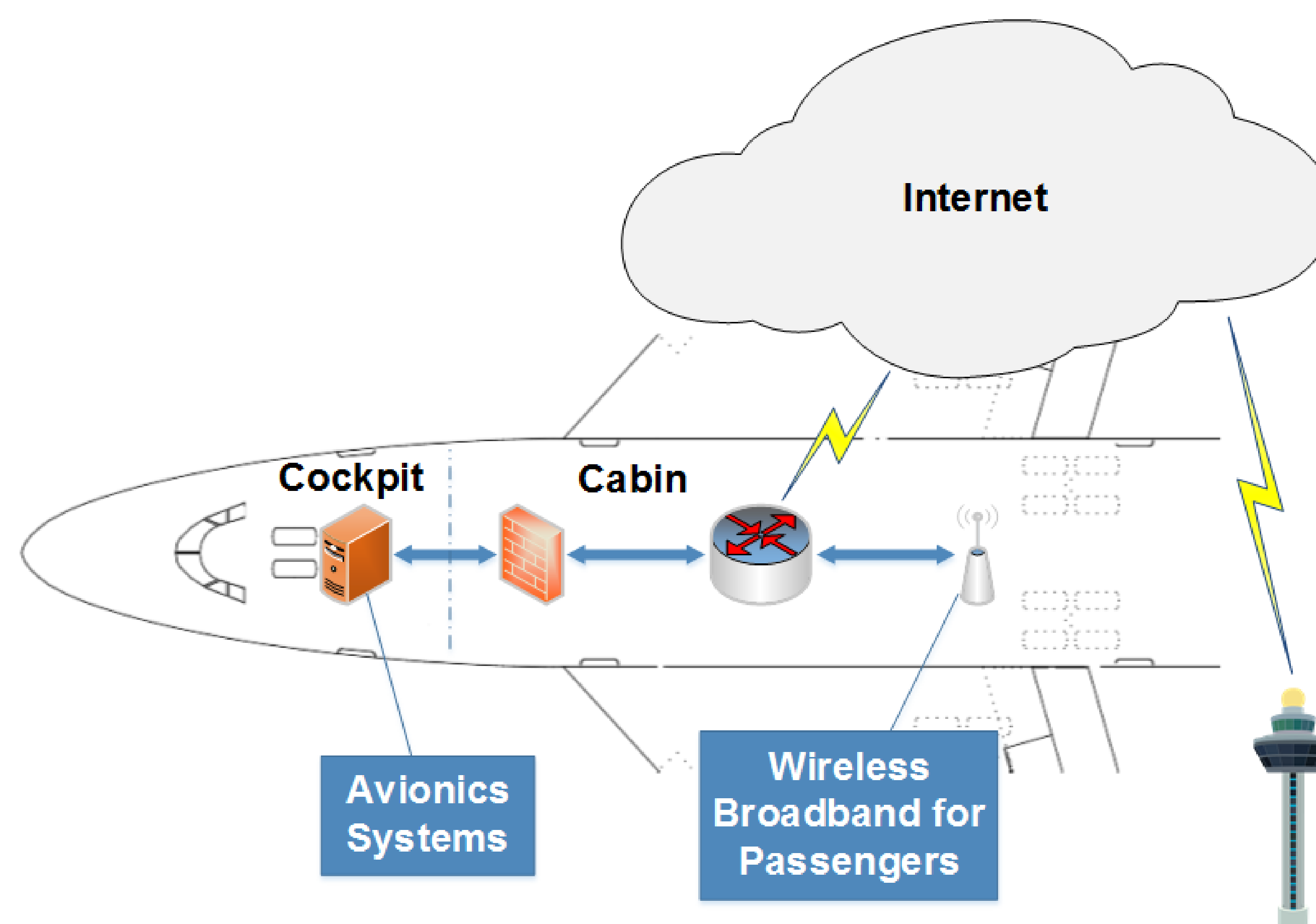
Vahid Heydari

Department of Electrical and Computer Engineering, The University of Alabama in Huntsville

Overview

according to GAO report, IP connectivity is increasingly used in aircraft systems, creating the possibility that unauthorized individuals might access and compromise aircraft avionics systems.

Using firewalls is a solution for protecting avionics systems located in the cockpit from intrusion by cabin-system users, such as passengers who use in-flight entertainment services onboard or even by someone on the ground.



Boeing uninterruptible autopilot:

Takes control of an aircraft away from the pilot or flight crew in the event of a hijacking through wireless connection between the aircraft and a ground station.

Prevent events like:

9/11 Attack, Malaysia Airlines Flight 370,
Germanwings Flight 9525

Problems:

- The technology would allow **cyber-terrorists** to hack into an airliner's controls.
- Zero-day exploits can defeat the best firewalls and IDSs.

KNOWING THE IP OF A VICTIM IS ENOUGH TO ATTACK

Solution: Dynamic IPs to prevent remote attacks.

Explanation

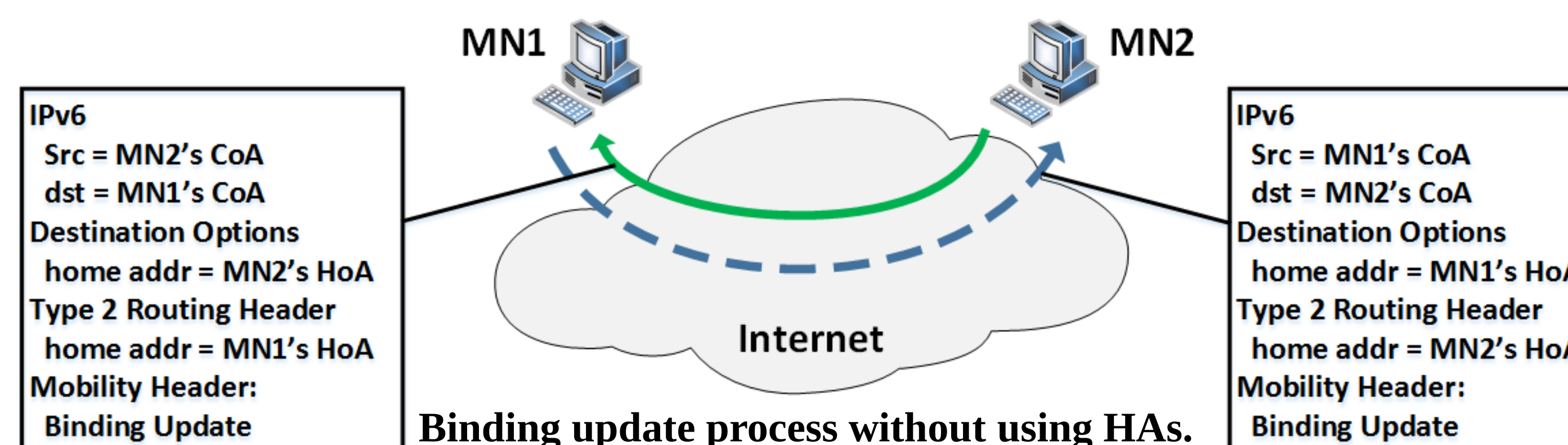
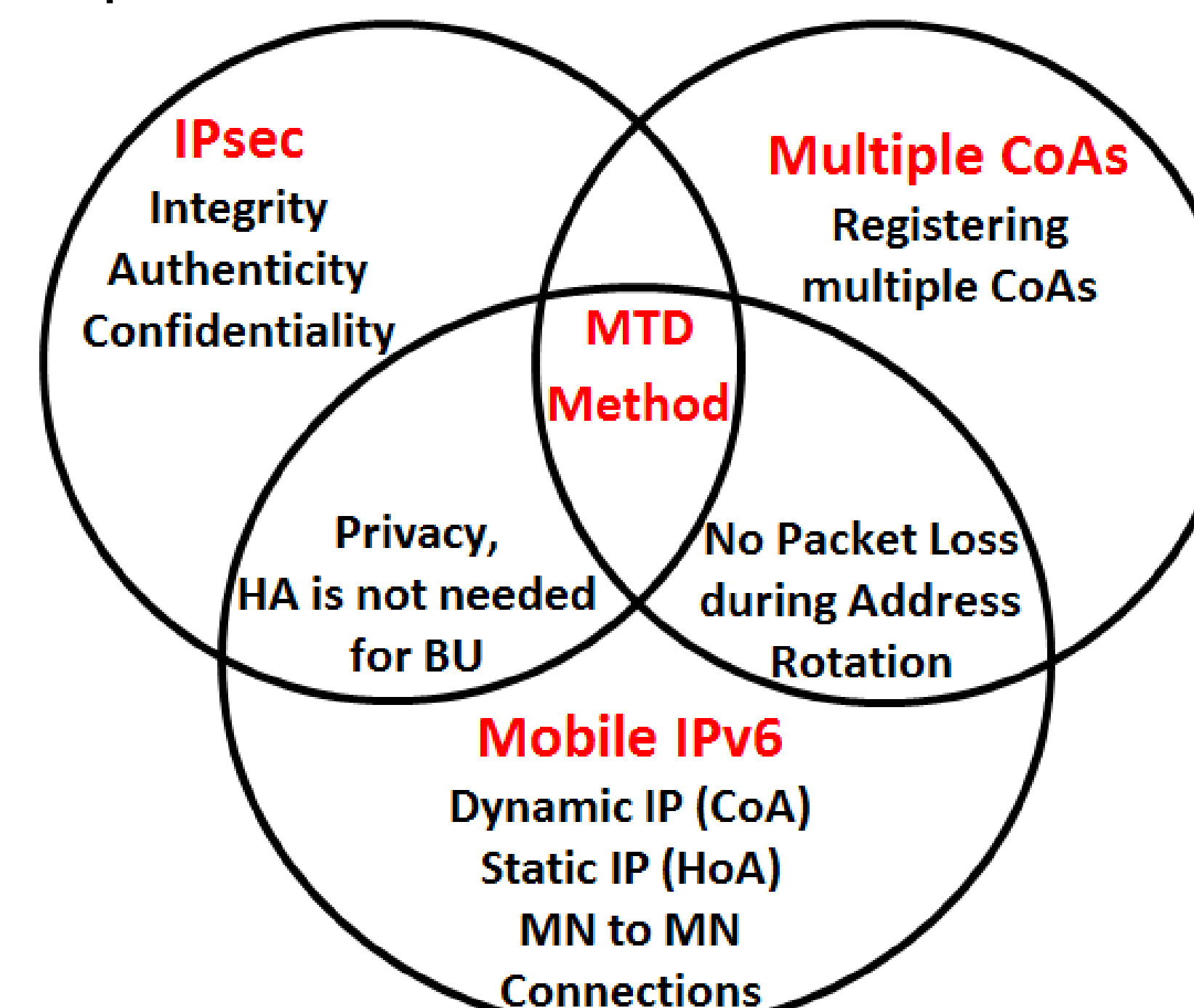
Mobile IPv6 is used when a Mobile Node (MN) is reached with a changing IP address as it moves through the network. Although we do not have any mobile nodes in our work, we treat peer nodes as mobile nodes. In Mobile IPv6, a MN has a permanent IP address, Home Address (HoA), assigned by the Home Agent (HA). A MN also has an alternate address, Care-of Address (CoA), which is used by others to reach the MN.

A pseudo-random IP address generator is used to dynamically change the CoA after each shuffling interval. A binding update message is sent to inform the peer node of the new CoA.

Using IPsec for route optimization and sending binding updates directly to the CoA of the peer node

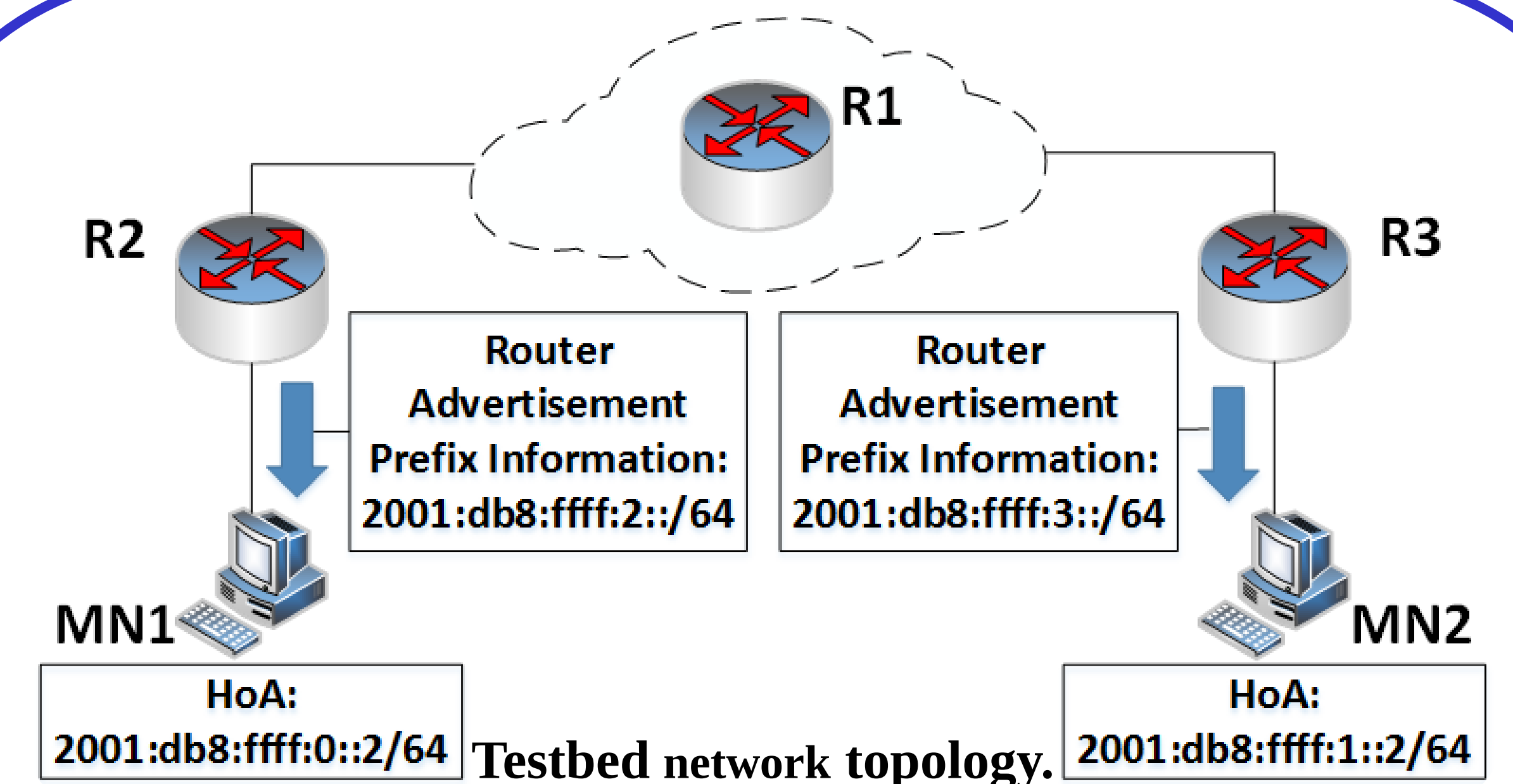
Home Agents are not needed

Permanent IPs (HoAs) are not accessible



Implementation Results

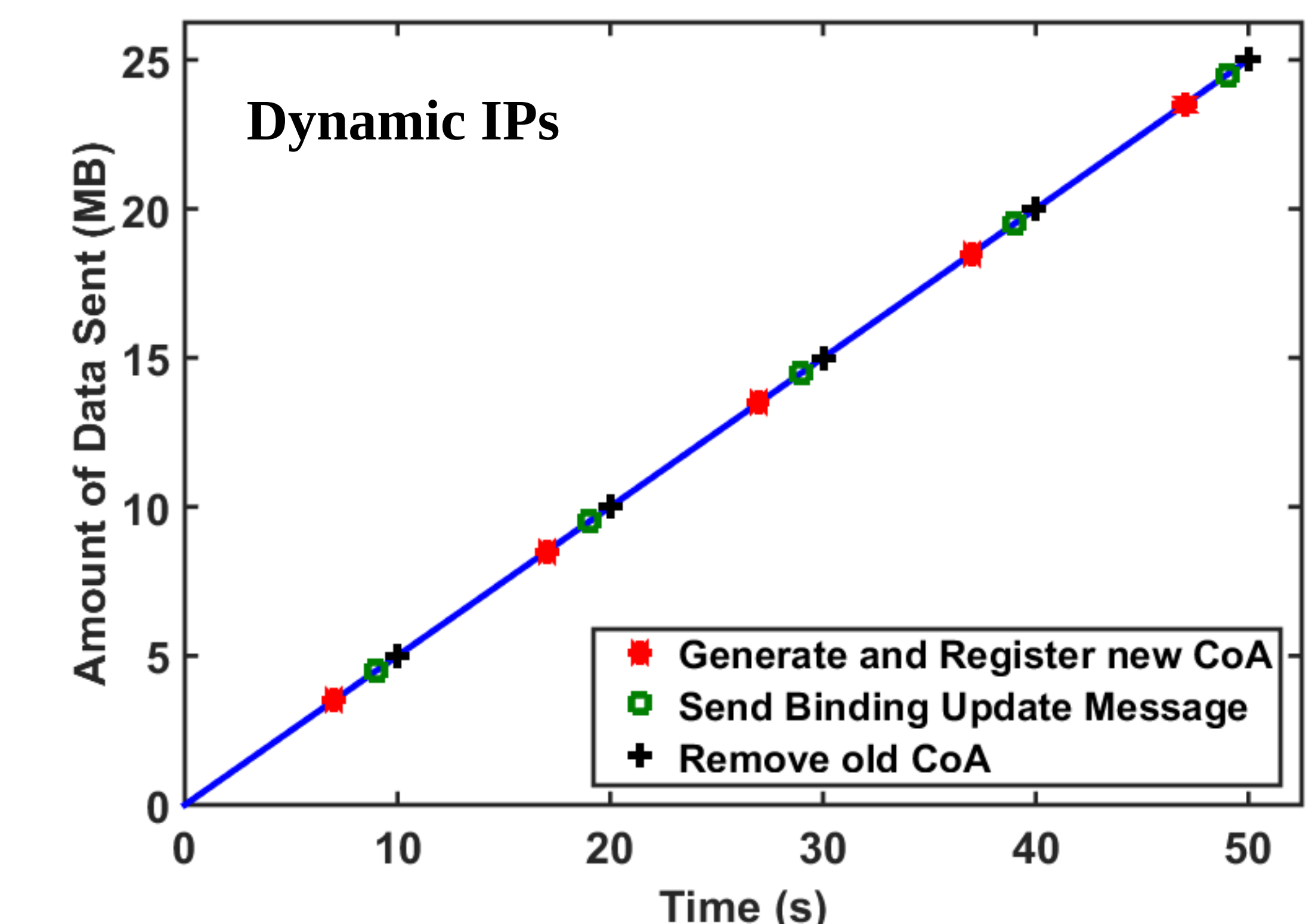
- Router R1 is used as the heart of the Internet. The WAN ports of R2 and R3 are connected to the LAN ports of R1.
- An implementation of Mobile IPv6 (UMIP) for Linux is used.
- The prefix of each HoA is different from the prefix received by route advertisement messages. So MNs think they are in a foreign network and register CoAs in this network.
- Current CoA of one MN should manually save in the peer MN that wants to start the route optimization.



During 50 seconds, MN1 sends 1000 TCP packets per second (each 500B) to MN2. Shuffling interval equals 10 seconds. **Same number of TCP packets** for dynamic IP and static IP. **Zero packet loss.**

Signaling Overhead (per update): 268B (two packets)

Data packet overhead (per packet): 24B (IPsec header)



Key Finding

Preventing remote attack from the first step (reconnaissance). Only peer nodes know the current accessible IPs (CoAs) of each other. IPsec provides Integrity, authenticity, confidentiality, and replay attack resistance (with IKE) for this method.

Acknowledgements

Thanks to Dr. Seong-Moo Yoo for assistance with this project.